Bastionado de Redes y Sistemas

Módulo Profesional 5022

Programación Didáctica 2025-2026

Curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información

Departamento de Informática y Comunicaciones

Profesores

Juanjo Felis
Teresa Martí Ferrando

I ES JAUME I I EL JUST
TAVERNES DE LA VALLDI GNA

Unió Europea
Fons Social Europeu
El FSE inverteix en el teu futur

GENERALITAT VALENCIANA
CONSELLERIA D'EDUCACIÓ

Departament d'Informàtica
Curs 2024-2025

Índice

Introducción

La programación didáctica ha de servir a los objetivos fundamentales de:

- Garantizar la unidad y coherencia de las enseñanzas que los distintos profesores del área o materia imparten en un mismo curso, asegurando que su práctica educativa se sustenta en unos principios educativos comunes dentro del área.
- Asegurar la continuidad de las enseñanzas correspondientes a una misma área o materia a lo largo de los distintos cursos.

Características del curso de especialización y del módulo profesional

El curso de especialización en **Ciberseguridad en Entornos de las Tecnologías de la Información** queda identificado por los siguientes elementos:

- Denominación: Ciberseguridad en Entornos de las Tecnologías de la Información.
- Nivel: Formación Profesional de Grado Superior.
- Duración: 720 horas.
- Familia Profesional: Informática y Comunicaciones.
- Rama de conocimiento: Ingeniería y Arquitectura.
- Créditos ECTS: 43.
- Referente europeo: P-5.5.4 (Clasificación Internacional Normalizada de la Educación - CINE-2011)[1].

El módulo **5022 Bastionado de Redes y Sistemas** pertenece al curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información. Este ciclo se regula en:

- Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional.
- Ley Orgánica 2/2006, de 3 de mayo, de Educación.
- Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.
- Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.
- RESOLUCIÓN de 15 de julio de 2020, de la Secretaría Autonómica de Educación y Formación Profesional, por la que se implantan determinados cursos de especialización de

[1] Categoría: Educación terciaria de ciclo corto vocacional. Subcategoría: Suficiente para la conclusión del nivel. https://www.educacionyfp.gob.es/dam/jcr:a60265fe-7b79-4b8b-a615-ace845e3ed1c/cine2011esp.pdf (Página 52)

Formación Profesional con carácter experimental en el curso académico 2020/2021, y se determinan su procedimiento de admisión y aspectos de la organización en el ámbito territorial de la Comunitat Valenciana.

El módulo profesional tiene una equivalencia de 10 créditos ECTS.

El módulo profesional de Bastionado de Redes y Sistemas (BRS), al cual hace referencia esta programación didáctica, está enmarcado dentro de las enseñanzas del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información. El Real Decreto 479/2020, de 7 de abril, establece los aspectos básicos del currículo para este curso de especialización que cuenta con un total de 720 horas de duración, de las cuales al módulo profesional de Bastionado de Redes y Sistemas le corresponden 168 horas, con una distribución de 7 horas semanales. Todo esto teniendo en consideración el Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

Competencia general del curso de especialización

Definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

Grupos del módulo

Durante el curso 2023/2024, en el que este curso de especialización se implanta de manera experimental, solo habrá un grupo, denominado 1CFEC, y será impartido presencialmente en turno diurno con horario vespertino. La docencia será conjunta entre los dos profesores asignados al módulo.

Competencias profesionales, personales y sociales

La formación del módulo contribuye a alcanzar las siguientes competencias profesionales, personales y sociales de este curso de especialización:

c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.

d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a

ataques.

e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

Objetivos

La formación del módulo contribuye a alcanzar los siguientes objetivos generales de este curso de especialización:

e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.

g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.

h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

Resultados de aprendizaje, criterios de evaluación y contenidos

Los resultados de aprendizaje, sus correspondientes criterios de evaluación y el contenido de este módulo se determinan en el Real Decreto 479/2020. A continuación tenemos una tabla donde se relacionan y se distribuyen entre las unidades didácticas.

Resultados de aprendizaje, criterios de evaluación y contenidos	**Unidades**
RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes. Criterios de evaluación: 1. Se han identificado los activos, las amenazas y vulnerabilidades de la organización. 2. Se ha evaluado las medidas de seguridad actuales.	UD 1. Introducción UD 2. Criptografía UD 3. Identidad y acceso UD 4. Bastionado de la red perimetral

3. Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización 4. Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular. 5. Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización. 6. Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización. Contenidos: Diseño de planes de securización: ● Análisis de riesgos. ● Principios de la Economía Circular en la Industria 4.0. ● Plan de medidas técnicas de seguridad. ● Políticas de securización más habituales. ● Guías de buenas prácticas para la securización de sistemas y redes. ● Estándares de securización de sistemas y redes. ● Caracterización de procedimientos, instrucciones y recomendaciones. ● Niveles, escalados y protocolos de atención a incidencias.	UD 5. Bastionado de la red corporativa UD 6. Bastionado del servidor
RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos. Criterios de evaluación: a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes. b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques. c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.	UD 2. Criptografía UD 3. Identidad y acceso UD 4. Bastionado de la red perimetral UD 5. Bastionado de la red corporativa UD 6. Bastionado del servidor

d) Se han definido protocolos y políticas de autenticación basados en *tokens, OTPs*, etc., en base a las principales vulnerabilidades y tipos de ataques. e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques. <u>Contenidos</u>: Configuración de sistemas de control de acceso y autenticación de personas: ● Mecanismos de autenticación. Tipos de factores. ● Autenticación basada en distintas técnicas:	
RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos. Criterios de evaluación: a) Se han identificado los tipos de credenciales más utilizados. b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto. c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio *web*. d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos. e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo *RADIUS - Remote Access Dial In User Servi* <u>Contenidos</u>: Administración de credenciales de acceso a sistemas informáticos: ● Gestión de credenciales. ● Infraestructuras de Clave Pública (PKI). ● Acceso por medio de Firma electrónica. ● Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red). ● Gestión de cuentas privilegiadas. ● Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.	UD 2. Criptografía UD 3. Identidad y acceso UD 4. Bastionado de la red perimetral UD 5. Bastionado de la red corporativa UD 6. Bastionado del servidor

RA4. Diseña redes de computadores contemplando los requisitos de seguridad. Criterios de evaluación: a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento. b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (*VLANs*). c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de *subnetting* para incrementar su segmentación respetando los direccionamientos existentes. d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (*routers*, puntos de acceso, etc.). e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas. <u>Contenidos</u>: Diseño de redes de computadores seguras: ● Segmentación de redes. ● Subnetting. ● Redes virtuales (VLANs). ● Zona desmilitarizada (DMZ). ● Seguridad en redes inalámbricas (WPA2, WPA3, etc.). ● Protocolos de red seguros (IPSec, etc.).	UD 4. Bastionado de la red perimetral UD 5. Bastionado de la red corporativa
RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad. Criterios de evaluación: a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad. b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico. c) Se han identificado comportamientos no deseados en una red	UD 6. Bastionado del servidor

a través del análisis de los registros (*Logs*), de un cortafuego. d) Se han implementado contramedidas frente a comportamientos no deseados en una red. e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización. Contenidos: ● Configuración de dispositivos y sistemas informáticos: ● Seguridad perimetral. Firewalls de Próxima Generación. ● Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall). ● Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware. ● Seguridad de entornos cloud. Soluciones CASB. ● Seguridad del correo electrónico ● Soluciones DLP (Data Loss Prevention) ● Herramientas de almacenamiento de logs. ● Protección ante ataques de denegación de servicio distribuido (DDoS). ● Configuración segura de cortafuegos, enrutadores y proxies. ● Redes privadas virtuales (VPNs), y túneles (protocolo IPSec). ● Monitorización de sistemas y dispositivos. ● Herramientas de monitorización (IDS, IPS). ● SIEMs (Gestores de Eventos e Información de Seguridad). ● Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: *NOCs* y *SOCs*.	
RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques. Criterios de evaluación: a) Se ha configurado la *BIOS* para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques. b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias. c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.	UD 6. Bastionado del servidor

d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos. e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad. Contenidos: ● Configuración de dispositivos para la instalación de sistemas informáticos: ● Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros. ● Seguridad en el arranque del sistema informático, configuración del arranque seguro. ● Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.	
RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques. Criterios de evaluación: a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema. b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos. c) Se ha incrementado la seguridad del sistema de administración remoto *SSH* y otros. d) Se ha instalado y configurado un Sistema de detección de intrusos en un *Host* (*HIDS*) en el sistema informático. e) Se han instalado y configurado sistemas de copias de seguridad. Contenidos: ● Configuración de los sistemas informáticos: ● Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.	UD 3. Identidad y acceso UD 4. Bastionado de la red perimetral UD 6. Bastionado del servidor

• Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.). • Eliminación de protocolos de red innecesarios (ICMP, entre otros). • Securización de los sistemas de administración remota. • Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.). • Configuración de actualizaciones y parches automáticos. • Sistemas de copias de seguridad. • Shadow IT y políticas de seguridad en entornos SaaS.	

Unidades didácticas y temporalización

El contenido de este módulo se define en:

> Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.

Y queda organizado como se describe en la siguiente tabla.

Unidades Didácticas	**Semanas**
UD 1. Introducción	1
UD 2. Criptografía	2
UD 3. Identidad y acceso	4
UD 4. Bastionado perimetral de la red	6
UD 5. Bastionado de la red corporativa	6
UD 6. Bastionado de servidores	7
Proyecto / ampliación / consolidación	4
Total	**30**

Metodología: orientaciones didácticas

Metodología general y específica

Las metodologías didácticas empleadas serán fundamentalmente procedimentales, basadas en la realización de ejercicios, tareas y prácticas, de forma que los contenidos teóricos del módulo pasan en un segundo plano, dándole mayor importancia a los contenidos procedimentales.
Además, las metodologías utilizadas (activas, colaborativas y cooperativas) están enfocadas al hecho de que los estudiantes sean los protagonistas de su propio aprendizaje.

Al inicio del curso escolar la persona coordinadora del Curso de Especialización realizará un presentación completa a los alumnos del curso. Tras la sesión de bienvenida, el profesorado encargado de cada módulo realizará la presentación correspondiente a dicho módulo. Por lo tanto los alumnos deben saber desde el inicio del curso qué contenidos van a impartirse, su temporalización, como van a ser evaluados, como van a ser los exámenes y las pruebas evaluativas, que tienen que hacer para superar el módulo y de qué forma pueden recuperar aquellas partes no superadas o la totalidad del módulo en su caso. También deben conocer la metodología de trabajo, cómo van a ser las sesiones en el aula, normativa de comportamiento en clase, de uso de los recursos materiales, etc.

Así mismo, y dada la heterogeneidad de estudios previos de los alumnos, el profesorado ha previsto unas sesiones iniciales de conocimientos previos para que todo el alumnado esté en disposición de poder seguir la dinámica de los contenidos de todos los módulos que forman el curso de especialización.

Respetando las particularidades de cada unidad didáctica, en la metodología general utilizada para desarrollar cada unidad seguiremos un orden como este.

- Explicación de los contenidos teóricos, con el apoyo de apuntes, presentaciones, pizarra o proyector. De cada concepto nuevo se tratará de explicar la utilidad y cómo realizarlo, y además, se intentará mostrar ejemplos de su uso en el mundo real. Es necesario que los alumnos encuentran la utilidad de los contenidos nuevos que van descubriendo para motivarse en su aprendizaje.

- Explicación práctica de los procedimientos asociados a conseguir las distintas capacidades que se fijan como objetivo. Es decir, los alumnos una vez han aprendido el concepto nuevo, deben saber utilizarlo, realizarlo, configurarlo o programarlo.

- Ejercicios sencillos que los alumnos deberán resolver.
- Explicación teórico-práctica de los conceptos y técnicas más avanzados.

- Ejercicios de consolidación para que resuelvan los alumnos.

- Actividades prácticas puntuables.

Al final de cada bloque o trimestre se realizará un control de validación de los contenidos desarrollados en las actividades prácticas puntuables.

Las tareas puntuables que debe realizar el alumno constan de actividades prácticas, ejercicios y problemas confeccionados por el profesor, y que deberán resolver en el aula, y entregar el resultado a través de la plataforma Aules.

En cuanto al trabajo del alumnado hay actividades individuales, actividades en pareja y actividades en pequeño grupo, y actividades que puedan simular metodologías de trabajo propias de la empresa. También se podrán plantear actividades en que los alumnos se dividen en dos grupos donde un grupo asume el rol de «atacantes» y el otro grupo de «defensores».

El material utilizado en el curso serán apuntes, presentaciones, videos, enlaces, etc., que el profesor pondrá a disposición de los alumnos a través de la plataforma Aules.

Se planteará al menos un proyecto de investigación en cada evaluación para que el alumno lo desarrolle de forma autónoma guiado por el profesorado del módulo.

Actividades y estrategias de enseñanza y aprendizaje

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo están relacionadas con:

- El diseño de planes de securización de la organización.
- El diseño de redes de computadores.
- La administración de los sistemas de control de acceso.

Evaluación

Tipos de evaluación

La evaluación es un componente básico en el proceso de enseñanza. Además, debe ser coherente con las características del Curso de Especialización, con los objetivos planteados y con la metodología utilizada. Por lo tanto, el aprendizaje del alumnado será evaluado de forma individual, continua, formativa e integradora. cuando el progreso de un alumno o alumna no sea el adecuado, se establecerán medidas de refuerzo educativo. estas medidas adoptarán en cualquier momento del curso, tan pronto como se detecten las dificultades y estarán dirigidas a garantizar la adquisición de las competencias imprescindibles para continuar el proceso educativo.

b) Criterios de evaluación

Los resultados de aprendizaje así como los criterios de evaluación vienen reflejados en el Real Decreto 479/2020, Anexo I.

c) Instrumentos de evaluación.

Con el fin de poder aplicar los criterios de evaluación a pruebas objetivas, tendremos en cuenta los siguientes instrumentos de evaluación.

- Actividades no puntuables: los alumnos deberán realizar pequeños ejercicios de menor entidad, los cuales serán corregidos y evaluados por el profesorado. Deberán realizarse correctamente para que el alumno pueda acogerse a las reglas de la evaluación contínua.

- Actividades prácticas puntuables: serán entregadas a través de la plataforma Aules. Se indicará en dicha plataforma que actividades forman parte de este grupo.

- Examen de validación: és un instrumento mediante el cual el profesorado pretende comprobar que el alumno ha realizado las actividades por su cuenta y sin copia o plagio.

- Proyecto de investigación: se propondrá algun proyecto a lo largo del curso.

d) Criterios de calificación y opciones de recuperación.

En la modalidad de evaluación contínua, la calificación que el alumno obtendrá en cada evaluación se obtendrá a partir del siguiente baremo:

- Examen / es de validación o de evaluación: 60%
- Prácticas puntuables en la plataforma Aules 20% (Media ponderada)
- Proyecto de investigación: 20%.

Aquí queda explicado con más detalle:

• Nota media del examen / es de validación o de evaluación que se realizan durante el transcurso de cada trimestre, con un peso del 60%. Tendrá que ser igual o superiores a 5, de lo contrario la evaluación quedará suspendida.

• Media ponderada de las notas de cada una de las prácticas que aparecen en la plataforma Aules como tareas. Esta nota tendrá un peso del 20% de la nota. Tendrá que ser igual o superiores a 4, de lo contrario la evaluación quedará suspendida. En la ponderación de la media se tendrá en cuenta el número de horas empleadas así como la dificultad técnica de la práctica.

• Las Evaluaciones se considerarán APROBADAS si el alumno obtiene una nota igual o superior a un 5.

• Entre 4 y 4.9, las evaluaciones constarán como Suspendidas, pero se podrá guardar la nota para realizar la media del Curso.

• La nota definitiva del módulo se obtendrá a partir de la media de la nota de las Evaluaciones, cada una deberá ser igual o superior a 4, siempre y cuando la nota del examen de dicha evaluación suspendida, sea mayor o igual a 5.

e) Recuperación de Evaluaciones

Las Prácticas entregadas fuera del plazo estipulado tienen una penalización en la nota de forma que puntuarán como máximo un 5 (apto) en caso de que se considere que está superada.

En caso de suspender una evaluación concreta, el alumno podrá ir a la convocatoria ordinaria de final de curso. A esta prueba, el alumno podrá ir de unidades o trimestres sueltos de una UD, o bien a todas, dependiendo de lo que le indique el profesor (será función del número de UD no superadas). Asimismo para considerarse Apto el alumno deberá entregar también los trabajos y prácticas pendientes que el profesor le indique.

La convocatoria extraordinaria constará de pruebas que aglutinan todas los temas. Por tanto, el alumno debe prepararse todos los Contenidos.

Se proporcionará un plan de recuperación para aquellos alumnos que no superen el curso a la convocatoria ordinaria y deban presentarse a la extraordinaria.

Recursos didácticos y organizativos

Se utilizarán distintas plataformas web y redes sociales. Aunque podrán emplear las que consideran más interesantes, se potenciará el uso de:

- aules.edu.gva.es - Aula Virtual de la CEICE (@ules).
- pages.github.com - GitHub Pages. Websites para ti y tus proyectos.
- www.google.es/edu - Google for Education del IES Jaume II
- twitter.com - Servicio de microblogging Twitter, Inc.
- es.linkedin.com - Comunidad profesional "on line"
- www.youtube.com - Publicador de vídeos Youtube
- edpuzzle.com - Lecciones con vídeos interactivos.
- Amazon Web Services - Plataforma servidores virtuales
- www.gns3.com Software de virtualización GNS3

Hay que destacar la importancia del aula virtual @ules como eje vertebrador del proceso de enseñanza-aprendizaje que recoge aspectos tan importantes como:

- La comunicación directa con los compañeros y el docente.
- Los recursos educativos.
- Las tareas a realizar.
- Actividades y recursos complementarios.
- Los productos finales entregados por el alumnado.
- Evaluación y calificación.

Es decir, el aula virtual complementará a la tradicional como lugar donde trabajar, exponer el trabajo realizado, compartir las dudas o ayudar a sus compañeros.

El profesorado aportará recursos y material didáctico tanto para la parte teórica como para la parte práctica. Por ejemplo:

- Prácticas y documentación desarrollados por el profesorado.
- Prácticas y documentación desarrollados por otros profesores.
- Publicaciones de universidades.
- Documentos de otras entidades y organizaciones.
- Otras recursos de Internet.

En estos recursos y materiales didácticos, además de los contenidos directamente relacionados con la materia, se incluirá de manera transversal otras contenidos como, por ejemplo:

- Educación en valores éticos y cívicos, como la igualdad.
- Promoción del emprendimiento, el espíritu de innovación y superación.

Por otro lado, respecto al hardware que usaremos, hay que destacar el uso de:

- Ordenadores de clase para trabajar con máquinas virtuales para reproducir varios escenarios que, por limitaciones técnicas y materiales, no se pueden montar en un entorno real.
- Plataformas de hosting y máquinas virtuales externas en el centro porque los alumnos tengan contacto con las herramientas reales que se pueden encontrar cuando acceden al mercado laboral.
- Dispositivos móviles (smartphones o tabletas) para estudiar y comprobar la seguridad.

Medidas de atención al alumnado con necesidades educativas específicas

Durante el presente curso, desde el servicio de psicopedagogía no se ha informado de ningún estudiante con necesidades educativas específicas, por lo que no será necesario aplicar medidas de atención para este tipo de estudiantes.

Previniendo la posible incorporación de alumnos con necesidades educativas especiales, el centro contempla una serie de medidas que se especifican a continuación.

- Cambios metodológicos.
- Prioridad en algunos objetivos y contenidos.
- Modificaciones en el tiempo de consecución de los objetivos.
- Adecuaciones en los criterios de evaluación en función de sus dificultades específicas.
- No obstante, su mayor o menor alejamiento del currículo básico dependerá de la evaluación y diagnóstico previo de cada alumno, a realizar por el Departamento de Orientación.

Las modificaciones en la programación del trabajo en aula, a través de la variedad de ritmos y actividades, permiten la atención individualizada a cada alumno. Constituyen, junto con la atención personalizada, el recurso de individualización más frecuente.

En términos generales, se contemplan dentro de este apartado todas aquellas medidas que se encaminan a diversificar el proceso de aprendizaje con arreglo a las diferencias personales de los alumnos y alumnas en cuanto a estilos de aprendizaje, capacidades, interés y motivaciones.